

# CONTENTS IN DETAIL

## FOREWORD

XIX

## ACKNOWLEDGMENTS

XXI

## INTRODUCTION

XXIII

What Embedded Devices Look Like . . . . .	xxiv
Ways of Hacking Embedded Devices . . . . .	xxv
What Does Hardware Attack Mean? . . . . .	xxv
Who Should Read This Book? . . . . .	xxvi
About This Book. . . . .	xxvii

## 1

## DENTAL HYGIENE: INTRODUCTION TO EMBEDDED SECURITY

1

Hardware Components. . . . .	2
Software Components. . . . .	4
Initial Boot Code. . . . .	5
Bootloader. . . . .	5
Trusted Execution Environment OS and Trusted Applications. . . . .	6
Firmware Images . . . . .	7
Main Operating System Kernel and Applications . . . . .	7
Hardware Threat Modeling. . . . .	7
What Is Security? . . . . .	7
The Attack Tree. . . . .	10
Profiling the Attackers. . . . .	10
Types of Attacks. . . . .	12
Software Attacks on Hardware . . . . .	12
PCB-Level Attacks . . . . .	15
Logical Attacks . . . . .	16
Noninvasive Attacks . . . . .	18
Chip-Invasive Attacks. . . . .	18
Assets and Security Objectives. . . . .	22
Confidentiality and Integrity of Binary Code. . . . .	23
Confidentiality and Integrity of Keys . . . . .	23
Remote Boot Attestation . . . . .	24
Confidentiality and Integrity of Personally Identifiable Information. . . . .	24
Sensor Data Integrity and Confidentiality . . . . .	25
Content Confidentiality Protection . . . . .	25
Safety and Resilience. . . . .	25
Countermeasures . . . . .	26
Protect . . . . .	26
Detect . . . . .	26
Respond. . . . .	27
An Attack Tree Example . . . . .	27
Identification vs. Exploitation . . . . .	30
Scalability . . . . .	30

Analyzing the Attack Tree . . . . .	30
Scoring Hardware Attack Paths . . . . .	31
Disclosing Security Issues . . . . .	33
Summary . . . . .	34

## 2

### REACHING OUT, TOUCHING ME, TOUCHING YOU: HARDWARE PERIPHERAL INTERFACES

**35**

Electricity Basics . . . . .	36
Voltage . . . . .	36
Current . . . . .	36
Resistance . . . . .	37
Ohm's Law . . . . .	37
AC/DC . . . . .	37
Picking Apart Resistance . . . . .	37
Power . . . . .	38
Interface with Electricity . . . . .	39
Logic Levels . . . . .	39
High Impedance, Pullups, and Pulldowns . . . . .	41
Push-Pull vs. Tristate vs. Open Collector or Open Drain . . . . .	42
Asynchronous vs. Synchronous vs. Embedded Clock . . . . .	43
Differential Signaling . . . . .	45
Low-Speed Serial Interfaces . . . . .	46
Universal Asynchronous Receiver/Transmitter Serial . . . . .	46
Serial Peripheral Interface . . . . .	48
Inter-IC Interface . . . . .	50
Secure Digital Input/Output and Embedded Multimedia Cards . . . . .	53
CAN Bus . . . . .	55
JTAG and Other Debugging Interfaces . . . . .	56
Parallel Interfaces . . . . .	59
Memory Interfaces . . . . .	60
High-Speed Serial Interfaces . . . . .	61
Universal Serial Bus . . . . .	62
PCI Express . . . . .	63
Ethernet . . . . .	63
Measurement . . . . .	64
Multimeter: Volt . . . . .	64
Multimeter: Continuity . . . . .	65
Digital Oscilloscope . . . . .	65
Logic Analyzer . . . . .	69
Summary . . . . .	70

## 3

### CASING THE JOINT: IDENTIFYING COMPONENTS AND GATHERING INFORMATION

**71**

Information Gathering . . . . .	72
Federal Communications Commission Filings . . . . .	72
Patents . . . . .	75
Datasheets and Schematics . . . . .	77
Information Search Example: The USB Armory Device . . . . .	79

Opening the Case . . . . .	86
Identifying ICs on the Board . . . . .	86
Small Leaded Packages: SOIC, SOP, and QFP . . . . .	88
No-Lead Packages: SO and QFN . . . . .	91
Ball Grid Array . . . . .	91
Chip Scale Packaging . . . . .	94
DIP, Through-Hole, and Others . . . . .	95
Sample IC Packages on PCBs . . . . .	95
Identifying Other Components on the Board . . . . .	98
Mapping the PCB . . . . .	102
Using the JTAG Boundary Scan for Mapping . . . . .	106
Information Extraction from the Firmware . . . . .	109
Obtaining the Firmware Image . . . . .	109
Analyzing the Firmware Image . . . . .	111
Summary . . . . .	118

## 4

### **BULL IN A PORCELAIN SHOP: INTRODUCING FAULT INJECTION 119**

Faulting Security Mechanisms . . . . .	120
Circumventing Firmware Signature Verification . . . . .	121
Gaining Access to Locked Functionality . . . . .	121
Recovering Cryptographic Keys . . . . .	121
An Exercise in OpenSSH Fault Injection . . . . .	122
Injecting Faults into C Code . . . . .	122
Injecting Faults into Machine Code . . . . .	123
Fault Injection Bull . . . . .	125
Target Device and Fault Goal . . . . .	126
Fault Injector Tools . . . . .	126
Target Preparation and Control . . . . .	127
Fault Searching Methods . . . . .	131
Discovering Fault Primitives . . . . .	132
Searching for Effective Faults . . . . .	135
Search Strategies . . . . .	142
Analyzing Results . . . . .	144
Summary . . . . .	146

## 5

### **DON'T LICK THE PROBE: HOW TO INJECT FAULTS 147**

Clock Fault Injection . . . . .	148
Metastability . . . . .	151
Fault Sensitivity Analysis . . . . .	154
Limitations . . . . .	154
Required Hardware . . . . .	155
Clock Fault Injection Parameters . . . . .	157
Voltage Fault Injection . . . . .	158
Generating Voltage Glitches . . . . .	158
Building a Switching-Based Injector . . . . .	159
Crowbar Injected Faults . . . . .	163
Raspberry Pi Fault Attack with a Crowbar . . . . .	164
Voltage Fault Injection Search Parameters . . . . .	171

Electromagnetic Fault Injection . . . . .	171
Generating Electromagnetic Faults . . . . .	173
Architectures for Electromagnetic Fault Injection . . . . .	175
EMFI Pulse Shapes and Widths . . . . .	176
Search Parameters for Electromagnetic Fault Injection . . . . .	177
Optical Fault Injection . . . . .	178
Chip Preparation . . . . .	178
Front-Side and Back-Side Attacks . . . . .	180
Light Sources . . . . .	181
Optical Fault Injection Setup . . . . .	183
Optical Fault Injection Configurable Parameters . . . . .	183
Body Biasing Injection . . . . .	184
Parameters for Body Biasing Injection . . . . .	186
Triggering Hardware Faults . . . . .	186
Working with Unpredictable Target Timing . . . . .	187
Summary . . . . .	188

## 6

### BENCH TIME: FAULT INJECTION LAB

**189**

Act 1: A Simple Loop . . . . .	190
A BBQ Lighter of Pain . . . . .	191
Act 2: Inserting Useful Glitches . . . . .	194
Crowbar Glitching to Fault a Configuration Word . . . . .	195
Mux Fault Injection . . . . .	210
Act 3: Differential Fault Analysis . . . . .	215
A Bit of RSA Math . . . . .	215
Getting a Correct Signature from the Target . . . . .	218
Summary . . . . .	222

## 7

### X MARKS THE SPOT: TREZOR ONE WALLET MEMORY DUMP

**223**

Attack Introduction . . . . .	224
Trezor One Wallet Internals . . . . .	224
USB Read Request Faulting . . . . .	226
Disassembling Code . . . . .	228
Building Firmware and Validating the Glitch . . . . .	229
USB Triggering and Timing . . . . .	233
Glitching Through the Case . . . . .	236
Setting Up . . . . .	236
Reviewing the Code for Fault Injection . . . . .	237
Running the Code . . . . .	240
Confirming a Dump . . . . .	241
Fine-Tuning the EM Pulse . . . . .	242
Tuning Timing Based on USB Messages . . . . .	242
Summary . . . . .	243

## 8

### I'VE GOT THE POWER: INTRODUCTION TO POWER ANALYSIS

**245**

Timing Attacks . . . . .	246
Hard Drive Timing Attack . . . . .	249
Power Measurements for Timing Attacks . . . . .	252

Simple Power Analysis . . . . .	253
Applying SPA to RSA . . . . .	254
Applying SPA to RSA, Redux . . . . .	256
SPA on ECDSA . . . . .	258
Summary . . . . .	264

## 9

### BENCH TIME: SIMPLE POWER ANALYSIS

**265**

The Home Lab . . . . .	266
Building a Basic Hardware Setup . . . . .	266
Buying a Setup . . . . .	269
Preparing the Target Code . . . . .	271
Building the Setup . . . . .	272
Pulling It Together: An SPA Attack . . . . .	275
Preparing the Target . . . . .	275
Preparing the Oscilloscope . . . . .	277
Analysis of the Signal . . . . .	278
Scripting the Communication and Analysis . . . . .	279
Scripting the Attack . . . . .	282
ChipWhisperer-Nano Example . . . . .	284
Building and Loading Firmware . . . . .	284
A First Glance at the Communication . . . . .	285
Capturing a Trace . . . . .	285
From Trace to Attack . . . . .	287
Summary . . . . .	291

## 10

### SPLITTING THE DIFFERENCE: DIFFERENTIAL POWER ANALYSIS

**293**

Inside the Microcontroller . . . . .	294
Changing the Voltage on a Capacitor . . . . .	295
From Power to Data and Back . . . . .	297
Sexy XORy Example . . . . .	299
Differential Power Analysis Attack . . . . .	300
Predicting Power Consumption Using a Leakage Assumption . . . . .	301
A DPA Attack in Python . . . . .	305
Know Thy Enemy: An Advanced Encryption Standard Crash Course . . . . .	308
Attacking AES-128 Using DPA . . . . .	310
Correlation Power Analysis Attack . . . . .	311
Correlation Coefficient . . . . .	312
Attacking AES-128 Using CPA . . . . .	316
Communicating with a Target Device . . . . .	321
Oscilloscope Capture Speed . . . . .	321
Summary . . . . .	322

## 11

### GETTIN' NERDY WITH IT: ADVANCED POWER ANALYSIS

**323**

The Main Obstacles . . . . .	324
More Powerful Attacks . . . . .	325
Measuring Success . . . . .	326
Success Rate-Based Metrics . . . . .	327
Entropy-Based Metrics . . . . .	328

Correlation Peak Progression . . . . .	329
Correlation Peak Height . . . . .	330
Measurements on Real Devices . . . . .	331
Device Operation . . . . .	331
The Measurement Probe . . . . .	334
Determining Sensitive Nets . . . . .	337
Automated Probe Scanning . . . . .	338
Oscilloscope Setup . . . . .	339
Trace Set Analysis and Processing . . . . .	342
Analysis Techniques . . . . .	342
Processing Techniques . . . . .	352
Deep Learning Using Convolutional Neural Networks . . . . .	355
Summary . . . . .	358

## 12

### BENCH TIME: DIFFERENTIAL POWER ANALYSIS

**361**

Bootloader Background . . . . .	362
Bootloader Communications Protocol . . . . .	362
Details of AES-256 CBC . . . . .	363
Attacking AES-256 . . . . .	364
Obtaining and Building the Bootloader Code . . . . .	365
Running the Target and Capturing Traces . . . . .	366
Calculating the CRC . . . . .	366
Communicating with the Bootloader . . . . .	367
Capturing Overview Traces . . . . .	367
Capturing Detailed Traces . . . . .	369
Analysis . . . . .	369
Round 14 Key . . . . .	370
Round 13 Key . . . . .	371
Recovering the IV . . . . .	374
What to Capture . . . . .	374
Getting the First Trace . . . . .	375
Getting the Rest of the Traces . . . . .	376
Analysis . . . . .	377
Attacking the Signature . . . . .	380
Attack Theory . . . . .	380
Power Traces . . . . .	381
Analysis . . . . .	381
All Four Bytes . . . . .	382
Peeping at the Bootloader Source Code . . . . .	383
Timing of Signature Check . . . . .	384
Summary . . . . .	386

## 13

### NO KIDDIN': REAL-LIFE EXAMPLES

**387**

Fault Injection Attacks . . . . .	387
PlayStation 3 Hypervisor . . . . .	388
Xbox 360 . . . . .	391
Power Analysis Attacks . . . . .	393
Philips Hue Attack . . . . .	393
Summary . . . . .	398

## THINK OF THE CHILDREN: COUNTERMEASURES, CERTIFICATIONS, AND GOODBYES

401

Countermeasures . . . . .	402
Implementing Countermeasures . . . . .	402
Verifying Countermeasures . . . . .	417
Industry Certifications . . . . .	420
Getting Better . . . . .	423
Summary . . . . .	423

## A

### MAXING OUT YOUR CREDIT CARD: SETTING UP A TEST LAB

425

Checking Connectivity and Voltages: \$50 to \$500 . . . . .	426
Fine-Pitch Soldering: \$50 to \$1,500 . . . . .	427
Desoldering Through-Hole: \$30 to \$500 . . . . .	429
Soldering and Desoldering Surface Mount Devices: \$100 to \$500 . . . . .	431
Modifying PCBs: \$5 to \$700 . . . . .	434
Optical Microscopes: \$200 to \$2,000. . . . .	435
Photographing Boards: \$50 to \$2,000 . . . . .	436
Powering Targets: \$10 to \$1,000 . . . . .	437
Viewing Analog Waveforms (Oscilloscopes): \$300 to \$25,000 . . . . .	437
Memory Depth . . . . .	439
Sample Rate . . . . .	439
Bandwidth . . . . .	441
Other Features . . . . .	443
Viewing Logic Waveforms: \$300 to \$8,000 . . . . .	443
Triggering on Serial Buses: \$300 to \$8,000 . . . . .	445
Decoding Serial Protocols: \$50 to \$8,000 . . . . .	445
CAN Bus Sniffing and Triggering: \$50 to \$5,000 . . . . .	447
Ethernet Sniffing: \$50. . . . .	447
Interacting Through JTAG: \$20 to \$10,000. . . . .	447
General JTAG and Boundary Scan . . . . .	447
JTAG Debug . . . . .	448
PCIe Communication: \$100 to \$1,000. . . . .	449
USB Sniffing: \$100 to \$6,000 . . . . .	450
USB Triggering: \$250 to \$6,000. . . . .	451
USB Emulation: \$100. . . . .	452
SPI Flash Connections: \$25 to \$1,000. . . . .	452
Power Analysis Measurements: \$300 to \$50,000 . . . . .	453
Triggering on Analog Waveforms: \$3,800+ . . . . .	456
Measuring Magnetic Fields: \$25 to \$10,000 . . . . .	457
Clock Fault Injection: \$100 to \$30,000 . . . . .	459
Voltage Fault Injection: \$25 to \$30,000. . . . .	460
Electromagnetic Fault Injection: \$100 to \$50,000 . . . . .	461
Optical Fault Injection: \$1,000 to \$250,000 . . . . .	461
Positioning Probes: \$100 to \$50,000 . . . . .	462
Target Devices: \$10 to \$10,000 . . . . .	463

**B**

<b>ALL YOUR BASE ARE BELONG TO US: POPULAR PINOUTS</b>	<b>467</b>
SPI Flash Pinout . . . . .	467
0.1-Inch Headers . . . . .	468
20-Pin Arm JTAG . . . . .	468
14-Pin PowerPC JTAG . . . . .	469
0.05-Inch Headers . . . . .	469
Arm Cortex JTAG/SWD . . . . .	469
Ember Packet Trace Port Connector . . . . .	470

**INDEX****471**